Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Навчально-науковий центр заочної форми навчання*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Дослідження корпоративної

мережі підприємства
(тема)

Виконав:
студент 2 курсу, групи *ІМІзм-20-1*
Артемчук В.О.
(прізвище, ініціали)

Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)

Тип програми *освітньо-наукова програма*

Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)

Керівник *доц. Скорик Ю.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2022 р.

.

Не містить відомостей заборонених до відкритого публікування

Студент / *Артемчук В.О.*/

Керівник  /*Скорик Ю.В.*/

Харківський національний університет радіоелектроніки
(повна назва вищого навчального закладу)
Навчально-науковий центр заочної форми навчання
Кафедра *Інформаційно-мережної інженерії*
Освітній рівень *другий (магістерський)*
Спеціальність *172 Телекомунікації та радіотехніка*
(код і назва)
Тип програми *освітньо-наукова програма*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«__25_» березня_____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Артемчук Вікторії Олександрівні*
(прізвище, ім'я, по батькові)
1. Тема роботи *Дослідження корпоративної мережі підприємства*

затверджена наказом університету від « *25* » *березня 2022 року № 34 Стз*
2. Термін подання студентом роботи до екзаменаційної комісії *17 травня 2022 р.*
3. Вихідні дані до роботи *Проектування корпоративної мережі клініки. Вибір мережного обладнання. Питання безпеки корпоративної мережі. Розподіл на VLAN.*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Принципи побудови корпоративної мережі
2. Мережні пристрої для побудови мережі
3. Маршрутизація та безпека
4. Розподіл мережі на VLAN
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____

Слайди у форматі Power Point (назва та мета кваліфікаційної роботи, актуальність роботи, вступ, узагальнена структура корпоративної мережі, вибір мережного обладнання, характеристики обладнання, маршрутизація та безпека корпоративної мережі, розподіл мережі на VLAN, висновки)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням.*	*25.03.22*	*виконано*
2	*Підбір літератури за темою роботи*	*26.03 – 30.03.22*	*виконано*
3	*Виконання розділу 1*	*31.03 – 12.04.22*	*виконано*
4	*Виконання розділу 2*	*13.04 – 23.04.22*	*виконано*
5	*Виконання розділу 3*	*24.04 – 06.05.22*	*виконано*
6	*Виконання розділу 4*	*07.05 – 13.05.22*	*виконано*
7	*Оформлення пояснювальної записки*	*14.05 – 17.05.22*	*виконано*

Дата видачі завдання *25 березня 2022 р.*

Студент _____ *Артемчук В.О.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Скорик Ю.В.*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 51 с., 12 рис., 6 табл., 16 джерел

Мета роботи – створити корпоративну мережу клініки.

В кваліфікаційній роботі розглянуто вирішення задачі дослідження і проектування корпоративної мережі. Зроблено вибір найбільш оптимальної технології, топології та мережного обладнання виходячи з технічних умов. Розглянуто основні технології реалізації корпоративної мережі.

КОРПОРАТИВНА МЕРЕЖА, ТОПОЛОГІЇ, КЛІНІКА, ВІДДІЛЕННЯ, ОБЛАДНАННЯ

THE ABSTRACT

Explanatory note: 51p., 12 fig., 6 tabl., 16 reference

The purpose of work – create a corporate network of the clinic.

In the qualification work the solution of the problem of research and design of the corporate network is considered. The choice of the most optimal technology, topology and network equipment based on technical conditions is made. The main technologies of corporate network implementation are considered.

CORPORATE NETWORK, TOPOLOGIES, CLINIC, DEPARTMENT, EQUIPMENT

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ISDN – Integrated Services Digital Network;

FDDI – Fiber distributed data interface;

LAN – Local Area Network;

IPsec – IP Security;

SSL – Secure Sockets Layer;

TLS – Transport Layer Security;

TCP – Transmission Control Protocol;

UDP – User datagram protocol;

OSI – Open Systems Interconnection model;

AH – Authentication Header;

ESP – Encapsulating Security Payload;

SA – Security Association;

SAKMP – security association and key management protocol;

SADB – Security Associations Database;

MTU – Maximum transmission unit;

SPD – Security Policy Database;

IGP – Interior Gateway Protocol;

OSPF – Open Shortest Path First;

VLAN – Virtual Local Area Network;

DHCP – Dynamic Host Configuration Protocol;

КМ – Корпоративна мережа.

ВСТУП

Будь-яке підприємство складається з сукупності взаємодіючих підрозділів, кожен з яких має свою особливість. Ці підрозділи взаємопов'язані функціонально, вони можуть проводити окрему діяльність у межах загального бізнес процесу, і ще інформаційну діяльність, тобто проводити обмін документами, розпорядженнями. Окрім того, ці елементи-підрозділи можуть взаємодіяти із зовнішньою системою. Ця взаємодія може бути інформаційною, функціональною.

При розвитку підприємства з’являється потреба у створенні максимально гнучкої та ефективної системи керування наявними підрозділами. З’являється потреба у забезпеченні якісного і надійного зв'язку між центральним офісом та всіма підрозділами, забезпеченні конфіденційності передавання даних, пониженню витрат на телекомунікаційне обладнання, витрачанні меншого часу на збір та обробку звітів, інформації, що циркулює між підрозділами.

Для підприємств чи організацій з віддаленими філіями вірне вирішення цих питань дає можливість успішного керування компанією, також дає можливість заощадити час і гроші. З досвіду величезних компаній можна сказати, що необхідно створити єдину інформаційну систему на базі корпоративної мережі.

Як результат еволюції комп'ютерної технології з'явилися гетерогенні комп’ютерні мережі, які є на основі обчислювальних мереж. Обчислювальна мережа, як складний комплекс взаємозв'язаних програмних та апаратних компонентів.

На підприємстві використовують обчислювальні мережі, щоб підвищити ефективність її роботи.

При використанні мережі проводиться і удосконалення комунікацій, тому що необхідно поліпшити процес обміна інформацією і взаємодії між працівниками підприємства, клієнтами і постачальниками

Тому, у даній кваліфікаційній роботі досліджується корпоративна мережа підприємства, її побудова та працездатність.

1 ЗАГАЛЬНІ ПРИНЦИПИ ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Корпоративна мережа

Корпоративна мережа (КМ) – це особливо складна система, яка необхідна для забезпечення передачі даних широкого спектру між різними застосуваннями, що використовуються у єдиній інформаційній системі організації. Узагальнена структура корпоративної мережі наведена на рис.1.1.

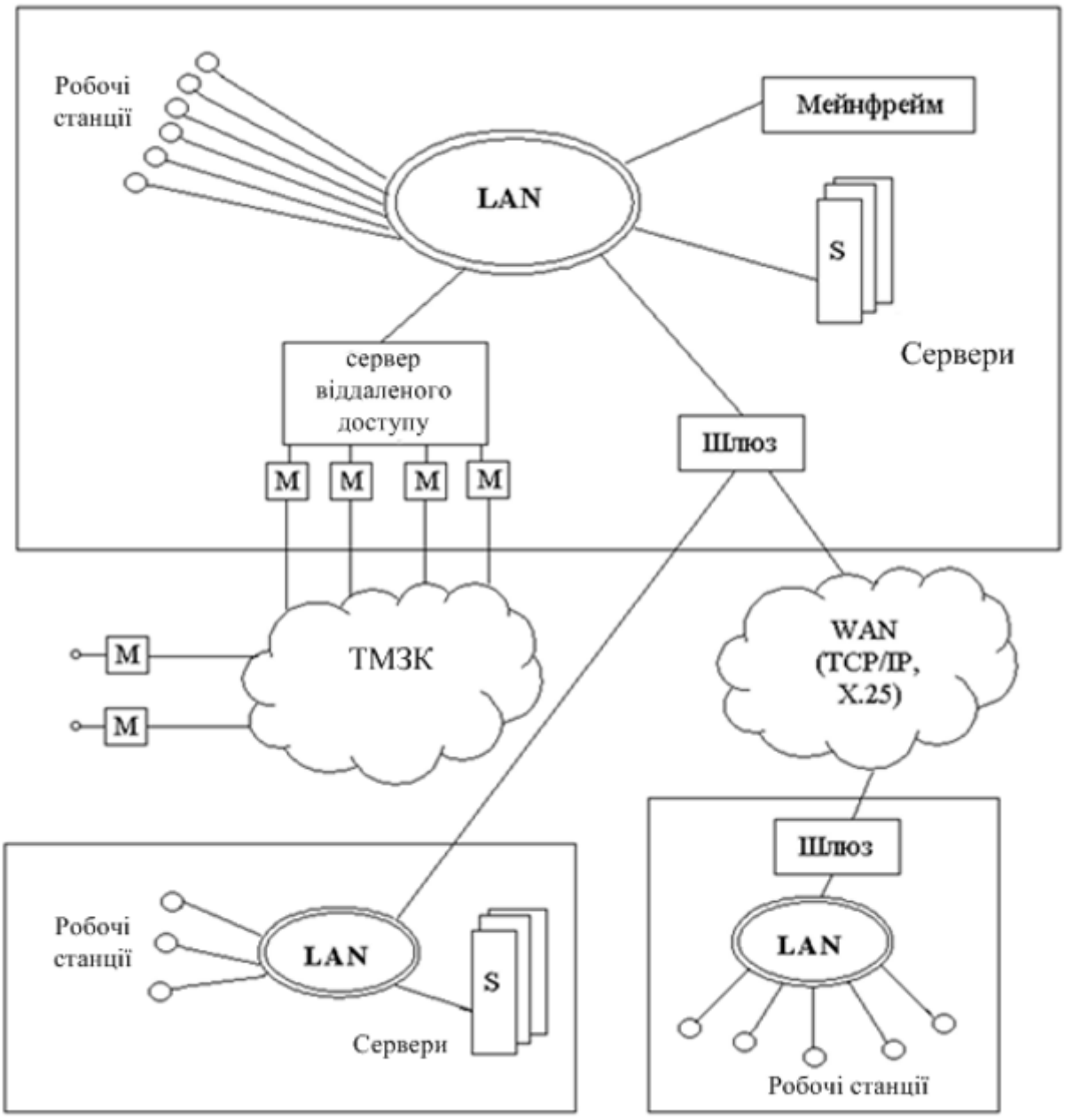

Рисунок 1.1 – Узагальнена структура корпоративної мережі

За допомогою КМ можна створити загальну, під усі підрозділи, базу даних, ведення електронного документообігу, організовувати селекторні наради і проводити відеоконференції із підрозділами, що знаходяться віддалено, забезпечувати всі необхідні потреби організації у високоякісному доступі до Інтернету і інших інтерактивних мереж. Все це впливає на зменшення часу реакції на зміни, що відбуваються в компанії, і забезпечується керування всіма процесами в реальному масштабі часу [1].

При цьому, менша залежність організації від операторів мобільного зв'язку. Часткова відмова від послуг цих операторів дає можливість істотно скоротити витрати організації. З'явилася можливість передавати будь-які конфіденційні дані з упевненістю, що ніхто, окрім уповноважених співробітників компанії, не має до них доступу.

Основним завданням системних інтеграторів і адміністраторів полягає у підтримці корпоративної мережі, її функцонуванні, щоб вся система якнайкраще виконувала обробку потоків інформації, циркулюючих між співробітниками підприємства і допомогала їм приймати своєчасно рішення. Оскільки життя не стає на місці, також і зміст корпоративної інформації, інтенсивність її потоків і способи її обробки постійно змінюються [1].

1.2 Етапи створення корпоративної мережі

Є декілька етапів створення корпоративної інформаційної системи:

- проведення інформаційного обстеження підприємства;
- за результатами обстеження обирається архітектура підсистеми і апаратно-програмні засоби її реалізації, за результатами обстеження можна обрати чи розробити необхідні компоненти інформаційної системи;
- система керування корпоративною базою даних;
- спеціальні програмні додатки і засоби;

- системи для підтримки ухвалення рішень.

Інформаційна система необхідна підприємству для забезпечення інформаційно-комунікаційної підтримки її функціонування. Проте спочатку необхідно зрозуміти цілі і завдання самого підприємства чи установи, що саме необхідно автоматизувати. А потім вже робити структуру та функціональне наповнення інформаційної системи [2].

Цілі інформаційного обстеження:

- формування та опис функцій кожного підрозділу організації, а також завдання, які вирішуються цим підрозділом;
- описування технології працювання кожного з підрозділів компанії та поняття того, що потрібно автоматизувати і у якій послідовності;
- описування технології працювання кожного підрозділу та інформаційних потоків, які з ним пов’язані;
- відображення технологій, визначення їх функціонального складу і кількості робочих місць у кожному підрозділі організації, а також описання функцій, які є на кожному робочому місці;
- описання загальних шляхів і алгоритмів проходження вхідних, внутрішніх та інших документів, а також технологій їх опрацювання [2].

Результатом обстеження є модель діяльності компанії, її інформаційна інфраструктура, на базі якої розробляється проект корпоративної інформаційної системи, вимоги до програмно-апаратного засобу та специфікації, на розробку прикладного програмного забезпечення [2].

1.3 Структура корпоративної мережі

Щоб підключити користувачі, що віддалені до корпоративної мережі можна за допомогою використання телефонного зв'язку. Там, де це можливо, можна використовувати мережі ISDN. Щоб об'єднати вузли мережі у більшості випадків необхідно використовувати глобальні мережі передачі

даних. Навіть там, де є можливість прокладки виділених ліній (наприклад, в межах одного міста) використання технологій пакетної комутації, що дає можливість зменшити кількість необхідних каналів зв'язку і забезпечення сумісністі системи з існуючими глобальними мережами [3].

Якщо потрібен доступ до відповідних послуг, то й необхідним є підключення корпоративної мережі до інтернет. Використовувати Internet як середовище передачі даних необхідно тільки тоді, коли інші засоби недоступні і фінансові міркування більше переважують вимоги надійності та безпеки. Якщо використання Internet тільки як джерела інформації, тоді краще користуватися технологією "з'єднання за запитом" (dial-on-demand), тобто це коли з'єднання з Internet відбувається тільки на потрібний час. Це значно знижує ризик несанкціонованого доступу до мережі ззовні [2].

1.4 Багатошарове представлення корпоративної мережі

Корпоративну мережу розглядають як складну систему, яка складається із взаємодіючих шарів. У основі мається шар комп’терного центру зберігання та обробки даних, і транспортна підсистема, яка забезпечує надійну передачу інформаційних пакетів між комп'ютерами [1-3].

- Над транспортною системою працюють мережні операційні системи, які організовують роботу додатків у комп'ютерах і надають через транспортну систему ресурси свого комп'ютера.

- Над операційною системою працюють різні застосування, проте через особливість задач систем керування базами даних, які зберігають основну корпоративну інформацію, цей клас системних застосувань відносять до окремого шару корпоративної мережі.

- На слідуючому рівні працюють системні сервіси, що надають кінцевим користувачам усю інформацію у більш зручній формі. Ці системи виконують деякі загальні для установ процедури обробки даних. Це може бути World Wide Web, система електронної пошти, система колективної праці.

- На верхньому рівні корпоративної мережі спеціальні програмні засоби, які виконують завдання, специфічні для цієї організації. Як приклади таких систем це системи автоматизації банку, автоматизованого проектування, керування технологічними процесами [3].

Стратегічні рішення, як правило, впливають на усю мережу у цілому, і зачепають кілька шарів, проте напочатку торкаються одного шару чи взагалі окремої підсистеми цього шару. Такий взаємний вплив рішень необхідно враховувати при плануванні технічної частини мережі, інакше можна зіткнутися з необхідною заміною, наприклад, мережної технології, через те, що програма, яка застосована і мається дефіцит пропускної спроможності для трафіку даних [2,3].

1.5 Канали зв'язку корпоративної мережі

При створенні корпоративної мережі необхідна організація каналів зв'язку. Канали зв'язку прокладають по лініям зв'язку із залученням складної електронної апаратури та кабелів зв'язку. За характером сигналів, що передаються канали можуть бути аналоговими чи цифровими, тобто на одній лінії зв'язку одночасно можна створити як аналогові, так і цифрові канали, що функціонують окремо. Для цього застосовують апаратуру для створення каналів [4].

1.6 Віртуальні мережі передачі даних

Якщо казати про приватні мережі, то ідеально було б створити канали зв'язку тільки на тих ділянках, де мається необхідність, і передавати по них будь-які мережні протоколи, які необхідні для працюючих застосувань. Є технології побудови мереж передачі даних, що дозволяють усередині організувати канали, які виникають у потрібний час і у необхідному місці. Такі канали мають назву віртуальних. Система, яка об'єднує видалені ресурси за допомогою віртуальних каналів, має назву віртуальна мережа. Існують дві

основні технології віртуальних мереж – мережі з комутацією каналів і мережі з комутацією пакетів. До мереж з комутацією каналів відносяться, наприклад ISDN. Мережі з комутацією пакетів представлені технологіями X.25, Frame Relay і ATM [3,4].

1.7 Побудова транспортної системи корпоративної мережі

Транспортна система дає основу для взаємозв'язаної роботи окремих комп'ютерів, тому транспортну систему зачасту плутають з самим поняттям "Корпоративна мережа". Транспортна система корпоративних мереж складається з ряду підсистем і елементів. Найбільш значними складовими транспортной системи є локальні та глобальні мережі організації, які розуміються як чисто транспортні засоби. Також локальна та глобальна мережі складаються з периферійних підмереж та магістралі, що ці підмережі пов'язує разом. Кожна підмережа також може мати структуру у вигляді ієрархії, яка створена своїми маршуртизаторами, комутаторами, концентраторами і мережними адаптерами. Все це комунікаційне обладнання пов'язане розгалуженою кабельною системою. Глобальні мережі, що об'єднують окремі локальні мережі також мають ієрархічну структуру з високошвидкісною магістраллю (як приклад, ATM), деякими периферійними мережами (як приклад, frame relay) та каналами доступу локальних мереж до глобальних [2-4].

При створенні та модернізації транспортної системи у питання її планування додають наступне.

- Створення транспортної інфраструктури для складних локальних мереж з продуктивністю, що масштабується.
- Вибір технології магістралі для великих локальних мереж організації. Технологія обирається використовуваними протоколами нижчого рівня, такими як Token Ring, Ethernet, Fast Ethernet, FDDI та суттєво впливає на типи використовуваного у мережі комунікаційного

обладнання. Магістраль це одна з найбільш дорогих частин у будь-якій мережі. І оскільки крізь неї проходить значна частина трафіку мережі, то її властивості вказуються практично на усіх сервісах корпоративної мережі, якими користуються кінцеві користувачі.

- Визначення структури магістралі. Цю структуру буде потім покладено у основу структури кабельної підсистеми, вартість якої може складати 15 і більше відсотку від всієї вартості мережі. Правильна структура магістралі повинна забезпечувати компроміс між якістю передачі трафіка (пропускна спроможність, затримка) і вартістю взагалі. Перш за все, на структуру магістралі найсильніше впливає обрана технологія, оскільки вона визначає максимальну довжину кабелю, можливість використовувати резервні зв'язки, типи кабелю і багато іншого [2-4].

1.8 Вибір технології та способи під'єднання підмереж

Обрання технології, структури зв'язків та комунікаційного обладнання для підмереж, що входять до локальних мереж. Відповідно для кожної підмережі це питання може вирішуватися з урахуванням вимог до кожного підрозділу організації [4].

Обрання способу об'єднання підмереж на магістралі може бути за допомогою маршрутизації, чи за допомогою шлюзів або ж транслюючих комутаторів. Якщо використовувати в усіх підмережах одну технологію, то потреба у трансляції протоколів може й відпасти і тому магістраль буде відрізнятись від підмереж тільки швидкістю та надійністю.

Після того, як зроблено вибір способу об'єднання підмереж обирається конкретний тип моделі комунікаційного обладнання [3,4].

1.9 Планування структури мережі

Комп'ютерна мережа – це декілька комп'ютерів у межах обмеженої території, які розташовані у одному приміщенні, чи близько розташованих

будинках і підключені до єдиної ліній зв'язку. На сьогодні більшість комп'ютерних мереж – це локальні комп'ютерні мережі (Local-Area Network), які зазвичай розміщаються усередині однієї будівлі та засновані на комп'ютерній моделі клієнт/сервер [2-4].

В моделі клієнт/сервер зв'язок по мережі поділяється на дві області: сторона клієнта та сторона сервера. По визначенню, клієнт дає запит на інформацію або послугу із сервера. Сервер обслуговуватиме запити клієнта. Найчастіше кожна сторона у моделі клієнт/сервер може виконувати функції і серверу, і клієнта. При проектуванні комп'ютерної мережі необхідно обирати різні компоненти, які дають можливість визначити, яке саме програмне забезпечення й обладнання можна використати при формуванні корпоративної мережі [4].

1.10 Вибір та обґрунтування топології мережі

Під топологією, за звичай, розуміється фізичне розташування комп’ютерів у мережі один щодо одного і засіб з’єднання їх лініями зв’язку. Необхідно відмітити, що поняття топології відноситься, перш за все, до локальних мереж, у яких структуру зв’язку можна легко простежети. У глобальних мережах, структура зв’язку зазвичай схована від користувачів і не дуже важлива. Тому, що кожен сеанс зв’язку може забезпечуватись за власним шляхом. Топологія визначає вимоги до обладнання, типу кабелю, що використовується, допустимі та найзручніші методи керування обміном, надійність роботи і можливості розширення мережі. Також важно відмітити чим фізична топологія мережі відрізняється від логічної [3-5].

Фізична топологія – це схема мережі, яка показує який ця мережа має вигляд у реальному світі, де і як які кабелі знаходяться, яке обладнання встановлено, яка довжина у кожного прольоту, який кабель у який порт увімкнено.

Логічна топологія мережі допомогає нам зрозуміти принцип функціонування даної мережі, визначити куди відправиться той чи інший запит і як комуніцює обладнання.

Найпростіша топологія – це point - to - point, точка до точки. Як правило, це два пристрої, які з'єднані між собою одним кабелем, які спілкуються між собою. Так раніш, це були пристрої, які з'єднувались за допомою модемів через телефонну лінію [3-5].

Наступна топологія має назву – Шина. Це, коли усі комп'ютери паралельно підключаються до однієї лінії зв'язку. Інформація від кожного ком'ютера одночасно передається усім іншим комп'ютерам. Тобто якийсь пристрій, який хоче з'єднатись з іншим пристроєм відправляє бродкаст повідомлення через дріт, де його чують усі. І пристрій, який ідентифікував себе як отримувач, відповідає повідомленням також усім.

Відмінною особливістю мережі по типу Шина, є наявність термінаторів з обох кінців дроту. А також під'єднання пристроїв за допомогою Т-коннекторів.

Переваги і недоліки даного типу мережі. Переваги – дуже легко налаштувати, легко розширювати мережу та обслуговувати. Доволі легко підключати нові пристрої. Потребує небагато кабелю. Проте є також і недоліки. Довжина кабелю – обмежена. Також обмежена кількість пристроїв, які можуть працювати у даній мережі. Усі пристрої залежать від центрального кабелю. Відповідно зрозуміти, де саме щось зламалось, дуже важко [5].

Продуктивність мережі доволі низька, коли до неї підключено багато пристроїв. Безпека цієї мережі доволі низька, тому що всі пристрої, що під'єднані до мережі прослуховують трафік, який передається.

На рис.1.1 зображена топологія Шина.

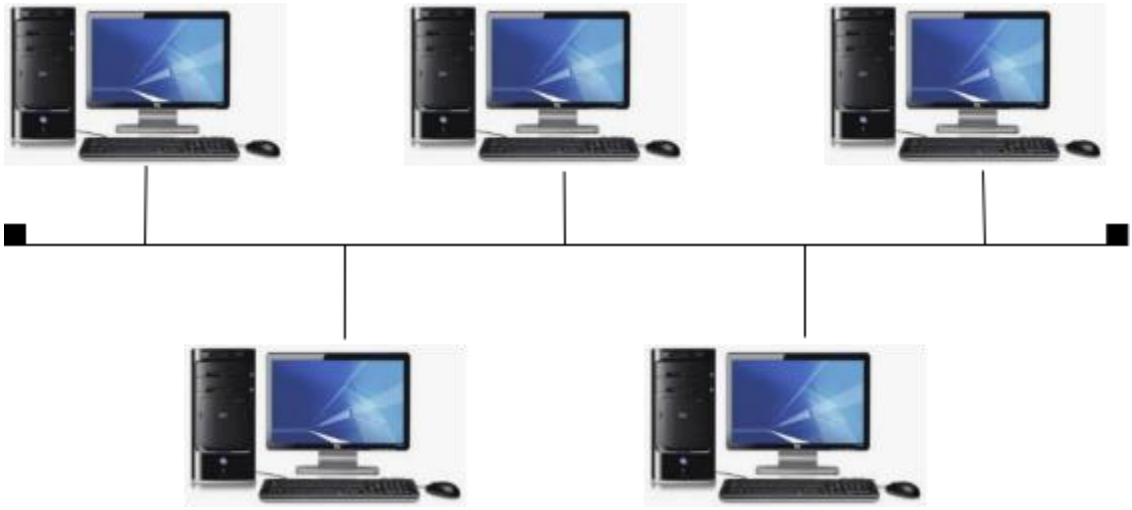

Рисунок 1.1 – Топологія шина

Наступка топологія – це Зірка. Це найбільш розповсюджена топологія на сьогодні. Усі пристрої під’єднуються до центрального вузла, який є ретранслятором. Це може бути свіч, хаб чи роутер. У наш час дана модель часто використовується у локальних мережах, коли до одного комутатора під’єднується декілька пристроїв і він є посередником у передаванні даних. У цій топології відмовостійкість набагато вище, ніж у попередніх топологіях. При пошкодженні кабелю перестає працювати тільки один пристрій і уся інша частина мережі продовжує працювати. Проте може бути пошкоджено центральний вузол і тоді уся мережа буде не дієздатною [5].

Переваги та недоліки даної топології. Почнемо з переваг. Дуже легко сконфігурувати і підпримувати даний тип мережі. Можна швидко виявити, чому саме пристрій не працює. Передача даних проводиться швидше і безпечніше. І будь-яка проблема на будь-якому з пристроїв ніяк не впливає на працездатність усієї мережі. Недолік даної топології – це залежність від центрального пристрою та від центрального кабелю. Також розмір даної мережі залежить від кількості портів на комутаторі. І відповідно працездастність даної мережі залежить від працездатності центрального

пристоя (комутатора чи хаба). І дана топологія потребує більшу кількість кабелей, тосу що кожен пристрій під’єднується окремим кабелем [3-5].

На рис. 1.2 зображена топологія Зірка.

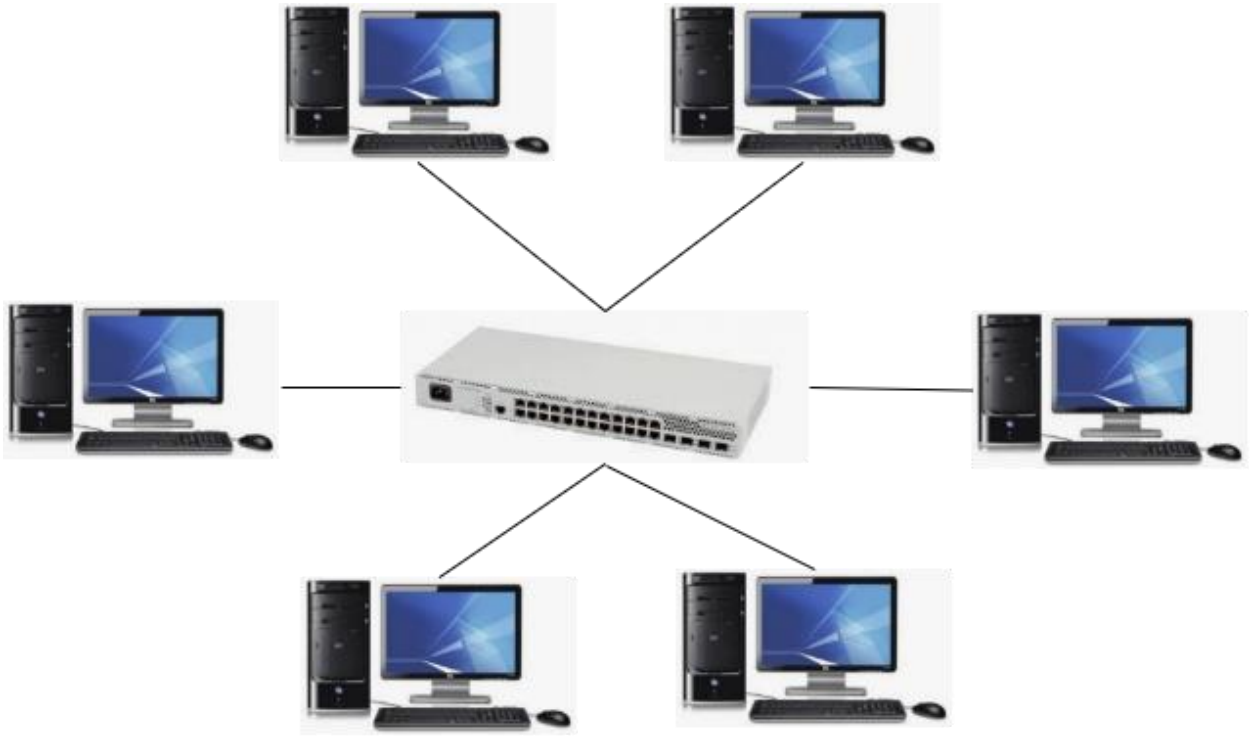

Рисунок 1.2 – Топологія Зірка

Наступна топологія – це Кільце. У даної топології кожен пристрій під’єднується до сусідніх пристроїв. Таким чином будується кільце. З однієї сторони комп’ютер приймає, з іншої – відправляє дані, тобто дані передаються по кільцю. Наступний комп’ютер є ретраслятором сигналу. Тому термінатори, як у топології Шина, не потрібні. Відповідно, якщо кабель десь пошкоджується, то кільце роз’єднується і мережа стає не працездатною [2-4].

Переваги та недоліки даної топології Кільце. Це дуже упорядкована мережа і це перевага. Дані передаються доволі швидко і додавання нових вузлів не впливає на працездатність мережі.

Тепер про недоліки, мережа залежить від кожного вузла. Відповідно, якщо ми захочемо додати чи видалити пристрій, то мережа буде непрацездатною. Дана топологія доволі повільніша ніж Ethernet. Тому доволі складно виявити у ній проблему, тому що не дуже зрозуміло на якому етапі вона з’являється. І відповідно, для того, щоб мережа працювала, усі комп’ютери повинні бути увімкнені [4].

На рис. 1.3 зображено топологію Кільце.

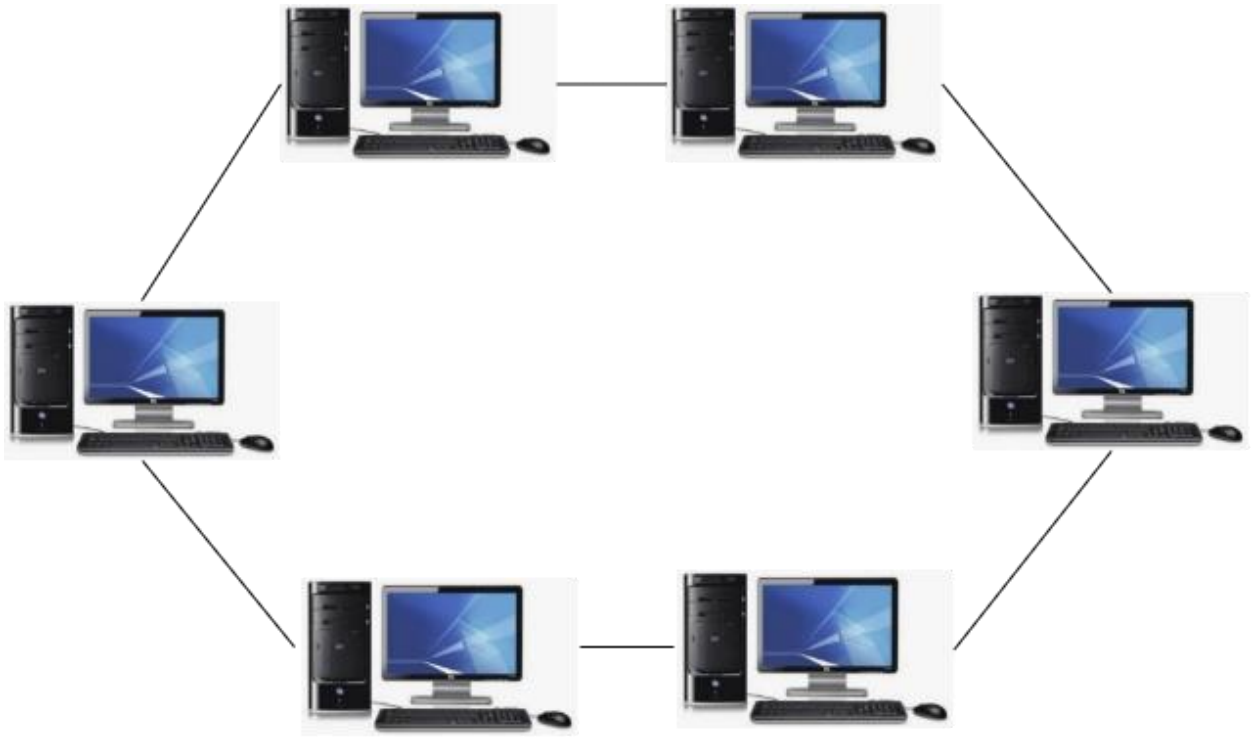

Рисунок 1.3 – Топологія кільце

Для підвищення працездатності мережі по типу Кільце, можна також застосовувати подвійне кільце, тобто у кожен пристрій підключено по два кабеля, а не один. Відповідно при відмові одного кабелю залишається працювати інший, резервний кабель. І таким чином, забезпечується додаткова працездатність мережі, а також збільшується швидкість передавання даних по мережі [4].

Наступний тип топології має назву – повнозв’язна топологія. Усі пристрої з’єднуються між собою на пряму. Даний тип моделі є найбільш відмовостійким, тому що не залежить від інших вузлів. На рис. 1.4 зображено повнозв’язну топологію.

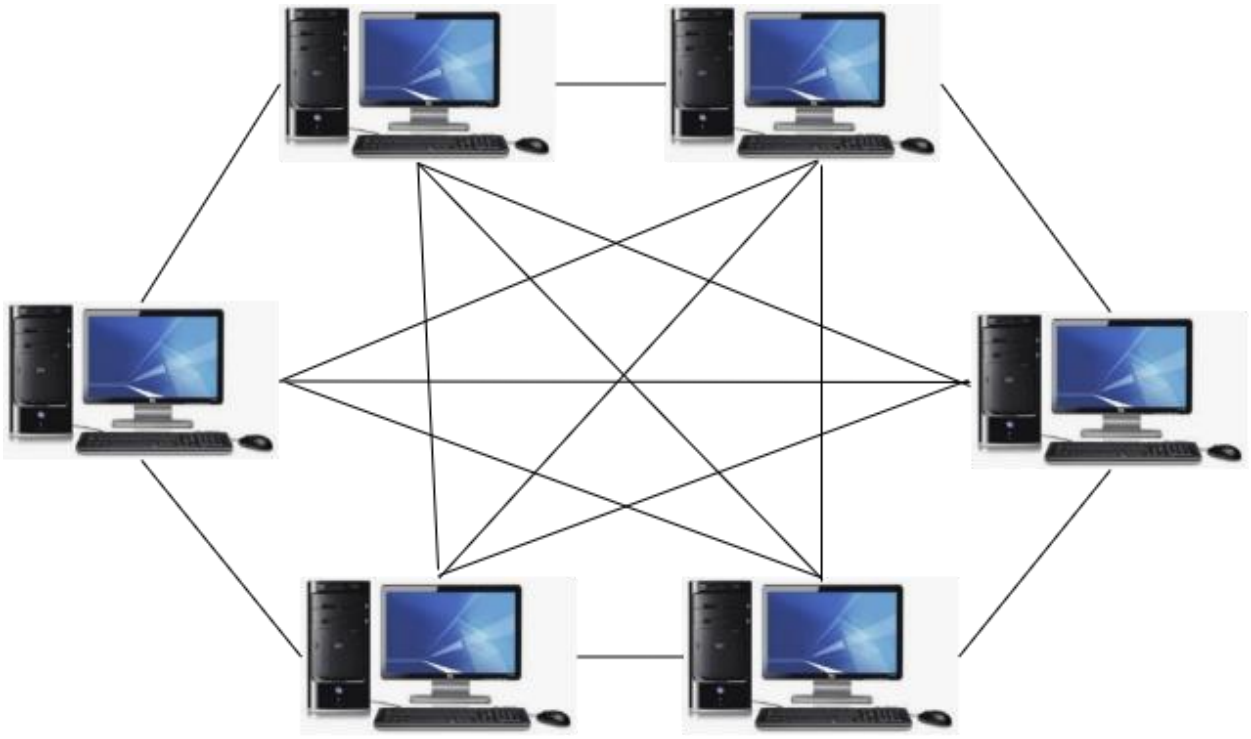

Рисунок 1.4 – Повнозв’язна топологія

Зробити повне налаштування мережі по такому типу топології дуже дорого і важко. Тому що, наприклад, у мережі з 1000 комп’ютерів необхідно підключити 1000 кабелей на кожен комп’ютер. Проте завадостійкість у цій мережі найбільш висока [4].

Якщо подивимось, як виглядає зв’язок між вузлами в мережі Інтернет, то побачимо топологію повнозв’язну.

Найбільш розповсюджена топологія – це гібрідна. Вона об’єднала у собі усі топології, які розглядали раніше. І має древовидну структуру. Вона є одною з найбільш відмовостійких топологій, тому що, якщо відбудеться обрив між двома з’єднаними топологіями, то не буде зв’язку тільки між цими топологіями, а всі інші об’єднані топології у мережі будуть працювати. На сьогодні дана топологія використовується у всіх середнії і велеких компаніях [3-5].

На рис. 1.5 зображено гібридну топологію.

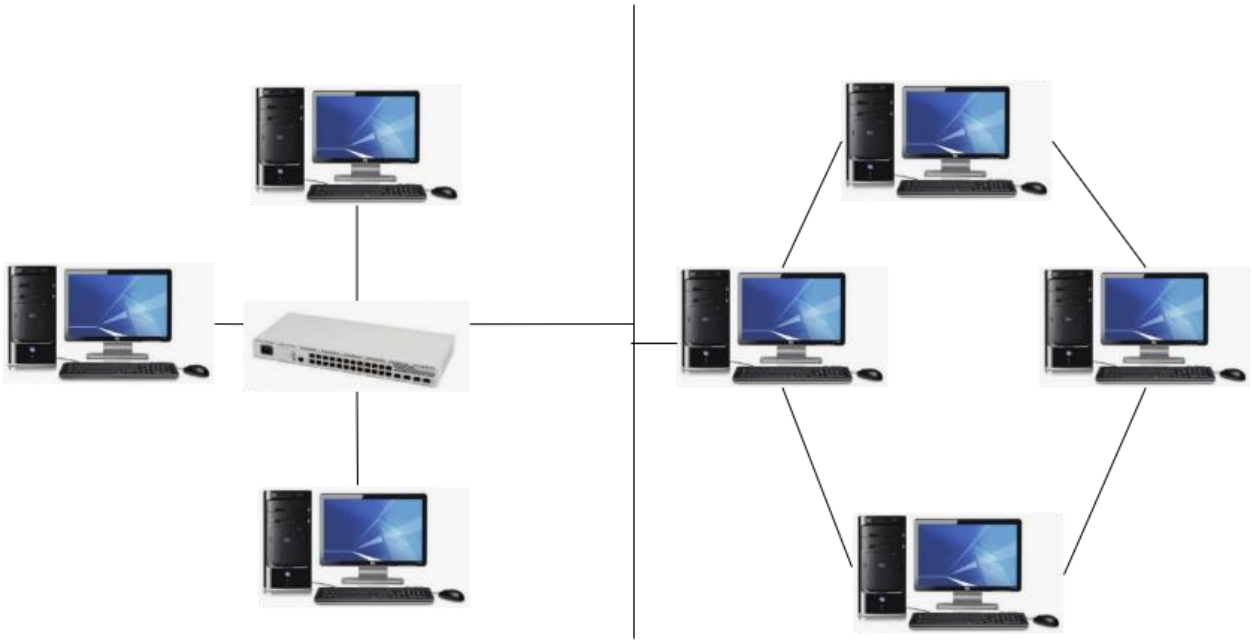

Рисунок 1.5 – Топологія гібридна

1.11 Адмініструваннння правами доступу

Кожне підприємство створює свої власні вимоги до проектування мережі, виходячи із певних вимог. Поперше визначається кількість користувачів, які будуть працювати у мережі. Від цього рішення залежать усі наступні етапи при створенні мережі.

Кількість робочих станцій напряму залежить від кількості співробітників. Також важлива і ієрархія компанії. Для організації із горизонтальною структурою, тобто усі працівники мають доступ до даних один одного, кращим рішенням є найпростіша однорангова мережа [2-4].

Компаніям, що побудовані за принципом вертикальної структури, у якої точно відомо, який співробітник і до яких даних має доступ, необхіден більш дорожчий варіант мережі – з виділеним сервером. Тільки у такій мережі є можливість адміністрування прав доступу.

2 МЕРЕЖНІ ПРИСТРОЇ ДЛЯ ПОБУДОВИ МЕРЕЖІ

Будуємо корпоративну мережу поліклініки з головним офісом у Харкові.

Маршрутизатор у головному відділенні буде Mikrotik CCR1036-12G-4S. Такий потужний маршрутизатор необхідено встановити для маршрутизування трафіку до головних серверів таких як 1С Підприємство, Asterisk, Windows Server 2016 Active Directory, та інших [6].

Комутатором в головному офісі обрано Mikrotik CRS326-24G-2S+RM для того, щоб розподілити мережу головного офісу на VLAN [7].

У філіалах обрано Mikrotik RB2011UiAS-2HnD-IN та комутатори MikroTik CSS326-24G-2S+RM – у цій ситуації комутатори другого рівня потрібні для запобігання «петлі» у мережі (блокування портів на яких була «петля»). На рис. 2.1 зображено маршрутизатор MikroTik CCR1036-12G-4S. У табл.2.1 наведені характеристики Mikrotik CCR1036-12G-4S [7, 8].

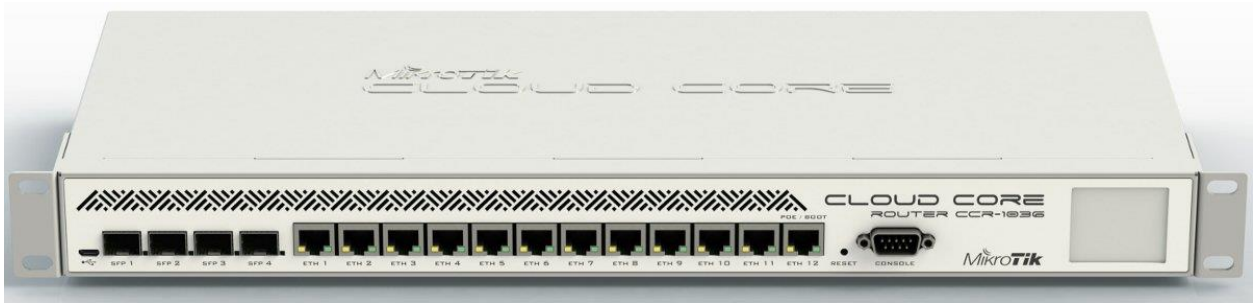

Рисунок 2.1 – Маршрутизатор MikroTik CCR1036-12G-4S

Таблиця – 2.1 Характеристики MIKROTIK CCR1036-12G-4SIII

Система	Характеристики
Процесор:	Tilera Tile GX 1200 MHz, 36 іядер
RAM:	4 GB DDR SDRAM
Flash:	1 GB NAND
Роз’єми	12 × 10/100/1000 Mbit/s Ethernet RJ45 Auto-MDI/X 4 × SFP cage Gigabit Ethernet (Mini-GBIC; SFP модуль не поставляється) 1 × DB9 RS232C asynchronous serial port 1 × microUSB port, host and device mode
Пропускна здатність	≤ 16 Гбіт/с
Швидкість маршрутизації	8 mpps standard 24 mpps fastpath
ОС:	MikroTik RouterOS Level6 (64 bit)
Інше	
Електроживлення	IEC C14 standard connector 110/220V (PSU included)
Розміри	55 × 145 × 355 мм
Споживання:	≤ 60 Вт

Макс. робоча температура:	50°C при 1.2 ГГц тактовій частоті 70°C при 1 ГГц тактовій частоті

На рис. 2.2 зображено комутатор CRS326-24G-2S+RM. У табл.2.2 наведені характеристики CRS326-24G-2S+RM.

Рисунок 2.2 – Комутатор CRS326-24G-2S+RM

Таблиця – 2.2 Характеристики CRS326-24G-2S+RM

Система	Характеристики
Процесор:	98DX3236A1-BTD4C000 800 MHz, 1 ядро
RAM:	512 MB
Flash:	16 MB
Роз’єми	24 × 10/100/1000 Mbit/s Ethernet with Auto-MDI/X 2 × SFP+ cage Gigabit Ethernet (Mini-GBIC; SFP модуль не поставляється, підтримуються модулі 1.25 Gb SFP і 10 Gb SFP+)

	1 × serial port RJ45
ОС:	MikroTik RouterOS Level 5 чи SwitchOS
Продовження табл. 2.2	
Додаткові фукції	
Управління пристроєм	WinBox, Web-інтерфейс
Інше	
Електроживлення	24 V, 1.2 A блок живлення у комплекті PoE in: 10-30V on Ether1
Споживання	≤ 24 Вт
Розміри	440 × 144 × 44 мм
Робоча температура	от -40°C до +60°C

На рис. 2.3 зображено маршрутизатор MikroTik RB2011UiAS-IN. У табл. 2.3 наведені характеристики Mikrotik RB2011UiAS-IN.

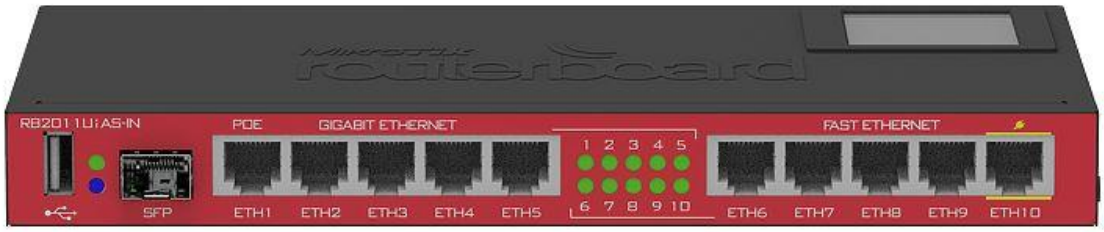

Рисунок 2.3 – Маршрутизатор MikroTik RB2011UiAS-IN

Таблиця – 2.3 Характеристики Mikrotik RB2011UiAS-IN

Система	Характеристики
Процесор	Atheros AR9344 600 MHz
RAM:	128 MB DDR SDRAM
Роз’єми	5 × 10/100/1000 Mbit/s Ethernet RJ45 Auto-MDI/X 5 × 10/100 Mbit/s Ethernet RJ45 Auto-MDI/X 1 × SFP cage Gigabit Ethernet (Mini-GBIC; SFP модуль не поставляється) 1 × USB type A
ОС	MikroTik RouterOS Level5
Модуляція	OFDM: BPSK, QPSK, 16 QAM, 64QAM DSSS: DBPSK, DQPSK, CCK
Антена	2×всеспрямовані антени, MIMO2×2

Посилення антени	4 дБи
Частоти	2,4 ГГц
Додатково	
PoE вихід	порт №10 (500 мА)
Продовження табл. 2.3	
Інше	
Електроживлення	Jack 8–28V DC; PoE: 8–28V DC on Ether1 (Non 802.3af)
Споживання:	до 8 Вт
Розміри:	230 × 90
Вага:	плата: 146 г
Робоча температура:	от -35°C до +65°C

На рис. 2.4 зображено комутатор MikroTik CSS326-24G-2S+RM. У табл. 2.4 наведені характеристики CSS326-24G-2S+RM [7].

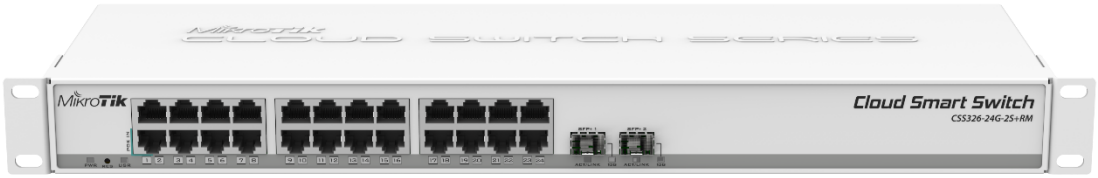

Рисунок 2.4 – Комутатор MikroTik CSS326-24G-2S+RM

Таблиця – 2.4 Характеристики MikroTik CSS326-24G-2S+RM

Система	Характеристики
Switch chip	98DX3216A1
Flash	2 MB
Раз’єми	24 × 10/100/1000 Mbit/s Ethernet with Auto-MDI/X 2 × 10G SFP+ порта. Підтримуються модулі 1.25G і 10G. (Mini-GBIC; SFP+ модулі не постачаються)
ОС	MikroTik SwOS
Додаткові функції	
Керування пристроєм	Web-інтерфейс
Інше	

Електроживлення	External 10-30V PSU included, Passive PoE input 10-30V
Споживання	≤ 19 Вт
Розміри	440 × 144 × 44 мм
Робоча температура	від -40°C до +70°C

3 МАРШРУТИЗАЦІЯ ТА БЕЗПЕКА

Оскільки в клініці багато філіалів, тому є необхідність під'єднати усі філіали і надати доступ до серверів, що знаходяться в центральному офісі – це місто Харків. Для цього необхідно використати IPsec тонель. Також для відмовостійкості використовується протокол OSPF, це протокол динамічної маршрутизації.

Протоколи IPsec, на відміну від таких популярних відомих протоколів SSL та TLS, функціюють на мережному рівні (третій рівень моделі OSI). Це дозволяє використовувати IPsec для захисту будь-яких протоколів, які базуються на TCP чи UDP. IPsec можна використувати для надання безпеки між двома IP-вузлами, між двома шлюзами безпеки чи між IP-вузлом та шлюзом безпеки. Протокол обробляє IP-пакети, що буди сформовані наступним способом, що описано нижче. IPsec дає можливість для забезпечення цілісності та конфіденційності даних, що передані по мережі [8,9].

IPsec використовує такі протоколи, щоб виконати різні функції:

- Authentication Header (AH) дає можливість зробити віртуальне з'єднання без втрат (даних, що передано), аутентифікацію джерела інформації і додаткову функцію, щоб запобігти повторну передачу даних.
- Encapsulating Security Payload (ESP) дає можливість забезпечити конфіденційність (шифрування) переданих даних, зробити обмеження потоку конфіденційного трафіку. Окрім всього, він має можливість забезпечити віртуальне з'єднання (переданих даних), аутентифікацію джерела даних і додаткову функцію із запобігання повторної передачі даних.
- Security Association (SA) забезпечують зв'язок алгоритмів та даних, що дають параметри, які необхідні для працювання AH чи ESP. Internet security association and key management protocol (ISAKMP) дає основу для аутентифікації та обміну ключами, перевірки аутентичності ключів.

Концепція "захищеного віртуального з'єднання" (SA, "Security Association") представляє собою фундамент у архітектурі IPsec. SA має симплексне з'єднання, що необхідне для передавання по ньому трафіка даних. При реалізації послуг з безпеки робиться SA на основі протоколів AH чи ESP (чи двох одночасно). SA відповідає концепції межтермінального з'єднання (point-to-point) і має можливість працювати у двох режимах: транспортний режим (РТР) та режим тунелю (РТУ). Транспортний режим працює при SA між двома IP-вузлами. У режимі тунелю SA робить IP-тунель [9].

Усі SA зберігаються у базі даних SADB (Security Associations Database) IPsec-модулю. Кожний SA має спеціальний маркер, що має три елементи:

- Індекс параметру безпеки (SPI)
- IP-адресу призначення

- Ідентифікатор протокола з безпеки (ESP чи AH)

IPsec-модуль, що має усі ці параметри, може знайти в SADB записи по конкретному SA. У список компонентів SA належать:

- Послідовний номер. 32-бітове значення, що необхідне для формування поля Sequence Number у заголовках AH чи ESP.
- Переповнення лічильнику порядкового номеру. Флаг, що сигналізує про переповнення лічильнику послідовного номеру.
- Вікно для відбиття атаки відтворення. Необхідне щоб визначити повторну передачу пакетів. Якщо значення у полі Sequence Number не додається у заданий діапазон, то пакет має бути знищеним.
- Інформація AH. Використовує алгоритм аутентифікації, також ключі, що необхідні, час життя ключів та багато інших параметрів [8,9].
- Інформація ESP. Використовує Алгоритм шифрування та аутентифікації, також необхідні ключі та параметри ініціалізації чи час життя ключів та багато інших параметрів.
- Режим працювання IPsec. Тунельний чи транспортний.

MTU. Максимальний розмір пакету, який є можливість передавати без фрагментації по віртуальному каналу [10].

Тому що захищені віртуальні з'єднання є симплексними, тому, щоб орнанізувати дуплексний канал, необхідні два SA. Окрім цього, кожному протоколу (ESP/AH) необхідно мати свою власну SA по кожному напрямку, тобто, для зв'язки AH+ESP необхідно чотири SA. Усі ці дані знаходяться у SADB.

У SADB містяться:

- AH: алгоритм автентифікації.
- AH: секретний ключ для автентифікації.
- ESP: алгоритм для шифрування.
- ESP: секретний ключ для шифрування.
- ESP: використання автентифікації (так/ні).

- Параметри для обмінювання ключами.
- Обмеження по маршрутизації.
- IP політика фільтрації [8-10].

Окрім бази даних SADB, реалізації IPsec надають базу даних SPD (Security Policy Database-База даних політик безпеки). Запис в SPD є з набора значень поля IP-заголовку та поля заголовку протокола верхнього рівню. Ці поля мають назву селектори. Селектори необхідні для фільтрування вихідних даних, щоб поставляти кожен пакет у відповідності з певним SA. Коли відбувається формування пакету, проводиться порівняння значень відповідних полів в пакетах (селекторні поля) з тими, що знаходяться у SPD. Потім знаходяться необхідні SA. Далі визначаються SA (у випадку, якщо вони є) для пакету і пов'язані з ним індекс параметру безпеки (SPI). Потім вже проводяться операції IPsec (це операція протоколів AH чи ESP) [10].

Приклади селекторів, що знаходяться у SPD:

- IP-адреси місця призначення.
- IP-адреси відправників.
- Протокол IPsec (AH, ESP або AH + ESP).
- Порти відправників і одержувачів.

Протокол OSPF. Остання версія протокола подана у RFC 2328. Протокол OSPF це протокол внутрішнього шлюзу (Interior Gateway Protocol — IGP). Протокол OSPF розповсюджує дані о вільних маршрутах між маршрутизаторами загальної автономної системи [8-10].

Властивості OSPF:

- Доволі висока швидкість збіжності.
- Відсутність обмежень по досяжності.
- Має підтримку мережних масок змінної довжини VLSM.
- Наявне оптимальне використання пропускної здатності мереж.
- Має оптимальне обирання шляху маршрутизації.

Згідно з RFC 2328 він незапатентований, маєть на увазі його відкрито для громадськості, такий же, як і протокол RIP. Проте OSPF на відміну від RIP, володіє значно більшою швидкістю збіжності, немає обмежень по довжині шляху 15 хопами, враховується пропускна здатність мережі при обиранні маршрута. Усе це зробило OSPF потужним протоколом маршрутизації, що масштабується [11].

На рис. 3.1 зображено загальну схему OSPF маршрутизації

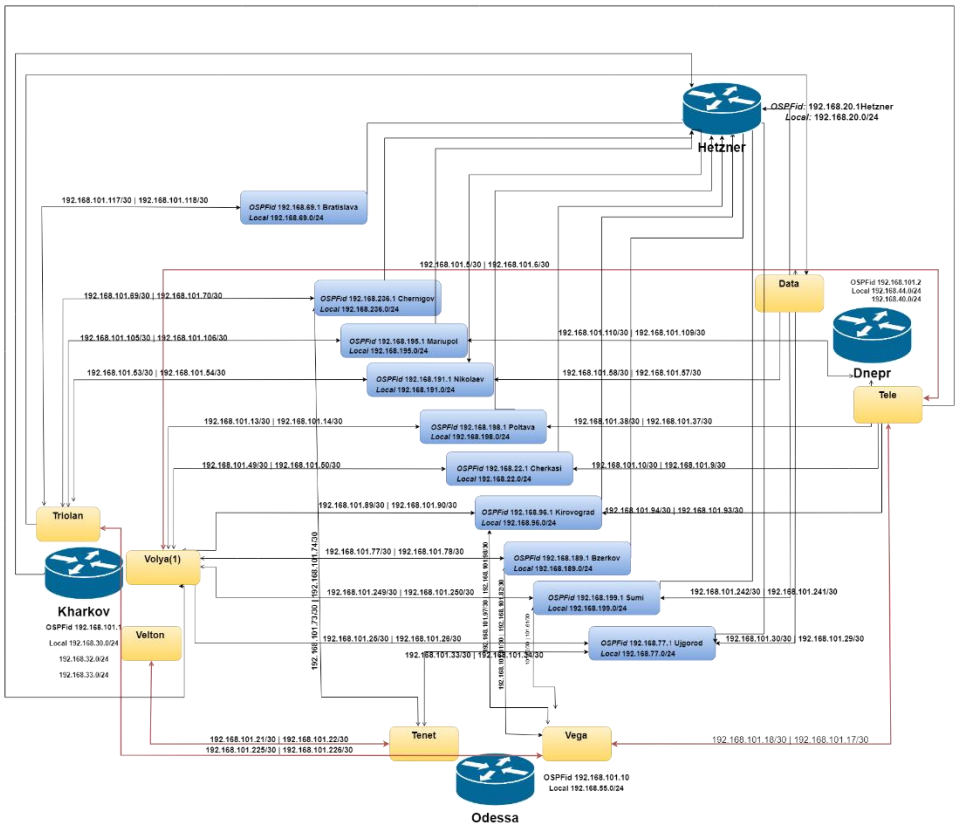

Рисунок 3.1 – Загальна схема OSPF маршрутизації по усіх відділеннях

Таким чином з’єднуються усі філіали та отримується одна загальна мережа. Проте для якісної безпеки і адміністрування необхідно розподілити мережу на підмережі «філіал-підмережа» і провести відокремлення загальної мережі, де будуть розташовані медичний персонал від підмережі адміністрування (Management VLAN), що наведено у табл. 3.1 [11, 12].

Таблиця 3.1 – Розподіл філіалів

Призначення	Підмережа	Коментарі
IPsec-тонель	192.168.101.0/24	Для зєднання філіалів
Харків	192.168.30.0/24	
Братислава	192.168.69.0/24	
Чернігів	192.168.236.0/24	

Продовження табл.3.1

Маріуполь	192.168.195.0/24	
Миколаїв	192.168.191.0/24	
Полтава	192.168.198.0/24	
Черкаси	192.168.22.0/24	
Кіровоград	192.168.96.0/24	
Біла Церква	192.168.189.0/24	
Суми	192.168.199.0/24	
Ужгород	192.168.77.0/24	
Дніпро	192.168.40.0/24	
Одеса	192.168.55.0/24	
Cloud	192.168.20.0/24	Сервер резервних копій та резервний Asterisk

4 РОЗПОДІЛ МЕРЕЖІ НА VLAN

VLAN (англ. Virtual Local Area Network – віртуальна локальна комп'ютерна мережа) – це група хостів із єдиним набором відповідних вимог, які взаємодіють так, ніби то додані до єдиного домену, незалежно як вони розташовані фізично. У VLAN ті ж самі атрибути, що і у фізичній локальній мережі, проте дає можливість кінцевим станціям бути взагалі разом, навіть коли вони не є на спільному мережному комутаторі. Зміни у мережі можуть бути зроблені завдяки програмному забезпеченню, щоб фізично не переміщати пристрої [12].

Якщо необхідно фізично скопіювати функції VLAN, тоді треба встановлювати окремий чи паралельний збір мережних кабелів та перемикачів, що знаходяться незалежно від первинної мережі. Але, VLAN розділює пропускну здатність; дві незалежних одно- гігабітних віртуальних мереж, що користуються одно-гігабітним зв'язком, мають зменшену пропускну здатність. Це віртуалізує VLAN (налаштування портів комутатору, позначки кадру на вході у мережу VLAN, пошук MAC таблиць) [12].

Віртуальні мережі це широкомовний домен мережі, що відокремлено і ізольовано на канальному рівні. Це логічна підмережа, що об’єднує пристрої з різних фізичних сегментів мережі. Віртуальні мережі об’єднують пристрої,

що взаємодіють між собою. Для організації такої взаємодії використовують роутери, що підвищує завантаженність мережі. Проте VLAN дозволяє вирішити дане питання за допомогою комутаторів. Також використання віртуальних мереж підвищує контроль і безпеку усередині мережі за рахунок обмеження доступу до внутрішніх ресурсів [12].

Під'єднання до VLAN може бути статичним чи динамічним. Під статичним розуміють перенаправлення порту мережного пристрою у ручну у певний VLAN. Коли користувач під'єднається до мережі через цей порт – він автоматично стає учасником віртуальної мережі. При зміні порту для під'єднання до тої ж мережі йому необхідно буде звернутися до адміністратора [12].

Динамічне під'єднання відбувається за участю певних програм і протоколів. Використовуючи сервер керування політикою VLAN адміністратор може розподіляти пристрої по віртуальним мережам на основі інформації якої він від них отримує, наприклад MAC адрес чи тип пристрою. У даному випадку коли користувач під'єднається через цей порт, порт зробить запит налаштувань від серверу і автоматично отримає номер VLAN по якому буде працювати. Незалежно від способу під'єднання кінцевий пристрій ніколи не буде знати, що він є членом VLAN [12].

VLAN створені, щоб забезпечувати послуги сегментації, даються маршрутизаторами у конфігуруванні з локальною мережею. VLAN, передбачають наступні питання, це й масштабованість, завадостійкість, безпека та керування мережею. Маршрутизатор, що знаходяться у топології VLAN забезпечує фільтрацію, дає безпечніть, узагальнення адресів і керування трафіку. Тому, що вимикачі не мають змоги з'єднувати IP-трафік з іншою мережею VLAN, тому що це розглядається як порушення єдності широкомовного домена VLAN.

Це важливо, коли треба створювати декілька мереж третього рівня на тому ж самому комутаторі другого рівня. Наприклад, коли сервер DHCP (що

перевірятиме його наявність) підключен до комутатора, то він обслуговуватиме хост, що налаштовано на отримання IP від серверу DHCP. За допомогою VLAN є можливість розділити мережі так, шоб вузли не мали змоги використати сервер DHCP та отримувати локальні адреси, чи отримувати адреси з другого сервера DHCP [12].

VLAN другого рівня конструкцій важливі, у порівнянні з IP-мережами, що мають конструкції третього рівня. При використованні VLAN, можна керувати пакетами даних трафіка та доволі швидко зреаговувати на переміщення. VLAN мережі дають гнучкість, щоб можно було адаптуватися до деяких змін в мережі деяким вимогам та дають можливість спрощеного адміністрування.

Стандарт IEEE 802.1Q це мережний стандарт, який забезпечує працездатність віртуальних мереж і Ethernet. Він описує принципи тегування Ethernet кадрів, а також процедури, що пов’язані з їх обробкою на мережних пристроях. Вставляється усередину Ethernet фрейму між полями мак адреси джерела і езертайп [12].

Розглянемо структуру VLAN Тегу детально на рис. 4.1.

Рисунок 4.1 – Структура VLAN Тегу

Розмір влан тегу складає 32 біти. Перші 16 займають Ethernet тайп з 16-річним значення 08100. Воно розташовується у не тегованих Ethernet фреймах у полі Ethernet тайп із значенням 08000. Таким чином мережне обладнання визначає чи є поле тегованим або не тегованим. Далі 3х бітне поле Priority code point, яке визначає рівень важливості даного фрейму. Після

нього йде одно бітовий Drop eligible індикатор, який може працювати разом з PCP чи окремо і показує можливість скидання даного фрейму у випадку з проблемами у мережі [12].

Останнє поле довжиною 12 біт це ідентифікатор віртуальної мережі. Він показує до якої даної віртуальної мережі належить фрейм. Перше і останнє значення даного поля є зарезервованим і недоступним для користувача. Таким чином користувач може працювати більш ніж 4000 віртуальними мережами.

Типи портів у віртуальних мережах. Перший тип – це код доступу, він працює з нетегованим трафіком і використовується для підключення пристроїв які не підтримують технології VLAN. Коли пристрій підключено і комутатор отримує від нього інформацію, то перше що він робить це тегує усі фрейми і потім відправляє їх до мережі. Коли інформація йде від мережі, то комутатор порівнює номер влан у фреймі зі своїм. Якщо вони співпадають, то видаляє тег і віддає дані на пристрій. Якщо вони не співпадають, то даний фрейм відкидається. Другий тип, це магістральні порти, які передають тегований трафік, вони використовуються для з'єднання пристроїв з підтримкою VLAN і для з'єдання комутаторів між собою. У комутаторах, крім налаштування портів, також можна створювати списки дозволених для комутації VLAN з яким буде зверятися трафік на магістральних портах. Дана функція підвищює безпеку і також дозволяє керувати трафіком у мережі [12].

У табл. 4.1 наведено розподіл мережі по VLAN у головному офісі медичної компанії.

Таблиця 4.1 – Розподіл мережі на VLAN у головному офісі

Менеджмент VLAN - 1	192.168.30.0/24	Сервери, маршрутизатор,

		керуючі комутатори
VLAN – 2 Мед. персонал	192.168.32.0/24	Маршрутизація тільки на БД пацієнтів, всі інші сервери ізольовано
VLAN – 3 керуючий персонал	192.168.33.0/24	Має доступ до 1С, Asterisk, FTP

ВИСНОВКИ

У даній кваліфікаційній роботі розроблено та проведено аналіз на працездатність корпоративної мережі поліклініки. Була розроблена корпоративна мережа із головним офісом у Харкові із серверами і дванадцятьма філіалами.

Наведено топології мереж і проведено їх аналіз.

Розглянуті питання щодо створення корпоративної мережі. Проведено обгрунтування вибору мережного обладнання, наведені їх характеристики. Обрано потужний маршрутизатор у головному відділенні Mikrotik CCR1036-12G-4S. Такий потужний маршрутизатор необхідно встановити для маршрутизування трафіку до головних серверів, таких як 1С Підприємство, Asterisk, Windows Server 2016 Active Directory, та інших.

Також у головному відділенні обрано комутатор Mikrotik CRS326-24G-2S+RM, для того, щоб розподілити мережу головного офісу на VLAN.

У філіалах обрано маршрутизатор Mikrotik RB2011UiAS-2HnD-IN та комутатори MikroTik CSS326-24G-2S+RM.

Розглянуті питання безпеки мережі на основі протоколу OSPF.

Зображено загальну схему OSPF маршрутизації. Проведено Розподіл мережі на VLAN.

ПЕРЕЛІК ПОСИЛАНЬ

1. Олифер В. Г. Компьютерные сети: Принципы, технологии, протоколы. – СПб.: Питер, 2005. – 864 с .
2. Степанов А.Н. Архитектура вычислительных систем и компьютерных сетей. – СПб: Питер, 2007. – 512 с.
3. Новиков Ю.В. Локальные сети. Архитектура, алгоритмы, проектирование. – М.: ЭКОМ. 2000 – 308
4. Таненбаум Э. Компьютерные сети. – СПб.: Питер. 2002. – 848 с.
5. Хелеби С. Принципы маршрутизации в Internet. – М: «Вильямс», 2001. – 448 с.
6. Спортак М. Компьютерные сети и сетевые технологии. – М.: ДиаСофт, 2005. – 711с.
7. Чигвинцева И.Р. Разработка на сети передачи данных ОАО «Таттелеком» сетевой инфраструктуры системы TR69. – «Вестник Казанского технологического университета». №13. 2012. – 230 с.
8. Построение коммутируемых компьютерных сетей: учебное пособие / Е.В. Смирнова и др. — М.: Национальный Открытый Универ- ситет «ИНТУИТ»: БИНОМ. Лаборатория знаний, 2011. – 367 с.
9. Гольдштейн Б.С. Сети связи: учебник для ВУЗов. – СПб.: БХВ – Петербург, 2010. – 400 с.
10. J. Eberspächer, H.-J. Vögel, C. Bettstetter, C. Hartmann. GSM – Architecture, Protocols and Services. Third Edition. – UK: John Wiley & Sons Ltd, 2009. – 327 pp.
11. Kappler C. UMTS Networks and Beyond. – UK: John Wiley & Sons Ltd, 2009. – 363 pp.
12. Мануал з налагодження OpenVPN [Електронний ресурс] – Режим доступу: https://openvpn.net/community-resources/how-to/